Monitoring Protokol Secure Socket Layer (SSL) menggunakan Wireshark

Annisa Cahyaningtyas
annisacahyaningtyas@gmail.com
http://annisacahyaningtyas.blogspot.com

Di era modern ini, bidang telekomunikasi sangatlah dibutuhkan hingga berkembang pesat, sebagai contoh yaitu internet. Dengan adanya internet, memberikan dampak yang besar dalam kehidupan kini atau pihak yang menggunakannya, seperti dalam hal melakukan tukar menukar data, komunikasi, transaksi via online, promosi, dan lainnya. Dengan demikian, hal tersebut berbanding lurus dengan tingkat kejahatan maya (dunia internet) pun meningkat.

Maka, agar pengguna internet tidak terganggu dan selalu merasa aman diperlukan sebuah solusi yang bisa membantu agar data yang dipertukarkan bisa aman dan bisa sampai ke tujuan, dan segala kegiatan lainnya, dan solusi yang ditawarkan adalah dengan menggunakan metode enkripsi yaitu suatu metode yang digunakan untuk mengamankan data dengan mengubah data asli ke dalam bentuk unicode dengan aturan tertentu. Ada beberapa metode enkripsi yang bisa digunakan diantaranya adalah dengan metode *Secure Socket Layer* (SSL).

1. Transport Layer Security (TLS) dan Secure Socket Layer (SSL)

Secure Socket Layer (SSL) dan Transport Layer Security (TLS), merupakan kelanjutan dari protokol kriptografi yang menyediakan komunikasi yang aman di Internet. SSL beroperasi pada layer transpor, menciptakan saluran enkripsi yang aman untuk data, dan dapat mengenkripsi banyak tipe data. Secure Sockets Layer, adalah metode enkripsi yang dikembangkan oleh Netscape untuk memberikan keamanan di Internet. SSL mendukung beberapa protokol enkripsi dan memberikan autentikasi client juga server.

Atau dapat dikatakan bahwa SSL merupakan Protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya. Berikut beberapa langkah dasar yang digunakan TLS dan SSL:

1. Melakukan perundingan (negoisasi) dengan ujung dari client atau server untuk dukungan algoritma.
2. Pengadaan Public key, *encryption-based-key*, dan *certificate-based authentication*
3. Melakukan proses enkripsi lalu lintas symmetric-cipher-based

Protocol SSL dan TLS berjalan pada layer di bawah application protokol seperti HTTP, SMTP and NMTP dan di atas layer TCP transport protocol, yang juga merupakan bagian dari TCP/IP protocol. Protokol SSL dan TLS dapat menambahkan keamanan ke protocol apa saja selama menggunakan TCP, dan kedua protokol tersebut paling sering terdapat pada metode akses HTTPS. HTTPS menyediakan keamanan web-pages untuk aplikasi seperti pada Electronic commerce. Protocol SSL dan TLS menggunakan cryptography public-key dan sertifikat publik key untuk memastikan dari identitas pihak yang dimaksud.

2. Kegunaan Secure Socket Layer (SSL)

SSL dirancang untuk mengamankan sesi web dan mempunyai banyak fitur lain, tetapi tujuan utamanya memang untuk mengamankan komunikasi melalui internet. SSL biasa digunakan untuk mengamankan protokol-protokol yang insecure menjadi secure.

SSL dijadikan perantara (penghubung) antara pemakai (user) dengan protokol HTTP yang kemudian menampilkan HTTPS kepada pemakai (client). Hal yang sama dapat dilakukan pula terhadap protokol-protokol insecure lain seperti POP3, SMTP, IMAP dan apa saja yang merupakan aplikasi TCP. SSL tidak memberi apa-apa kecuali handshake dan enkripsi. Diperlukan aplikasi untuk membuat SSL menjalankan tugasnya. Tanpa adanya traffic dari suatu aplikasi, SSL tidak melakukan apa-apa

3. Cara Kerja SSL

Cara kerja SSL dapat dilihat melalui tahapan – tahapan berikut :

1. Pertama, client membentuk koneksi awal ke server kemudian meminta koneksi SSL.
2. Bila server yang dihubungi telah dikonfigurasi dengan benar, maka server ini akan mengirimkan client *public key* miliknya ke client.
3. Client membandingkan sertifikat dari server ke *basisdata trusted authorities*. Bila sertifikat ini terdaftar di situ, artinya client mempercayai (trust) server itu dan akan lanjut ke langkah selanjutnya.
4. Lalu, client menggunakan *Public Key* yang didapatnya untuk men-enkripsi sesi dan mengirimkan *session key* ke server. Bila server meminta sertifikat client di langkah pengiriman public key (2), maka clent harus mengirimkannya sekarang.
5. Dan bila server di-setup untuk menerima sertifikat, maka server akan membandingkan sertifikat yang diterimanya dengan basisdata *trusted authorities* dan akan menerima atau menolak koneksi yang diminta.
    a. Bila kondisi ditolak, suatu pesan kegagalan akan dikirimkan ke client.
    b. Bila koneksi diterima, atau bila server tidak di-setup untuk menerima sertifikat, maka server akan men-decode *session key* yang didapat dari client dengan privete key milik server dan mengirimkan pesan berhasil ke client yang dengan demikian membuka suatu *secure data chanel.*

4. Implementasi dari SSL

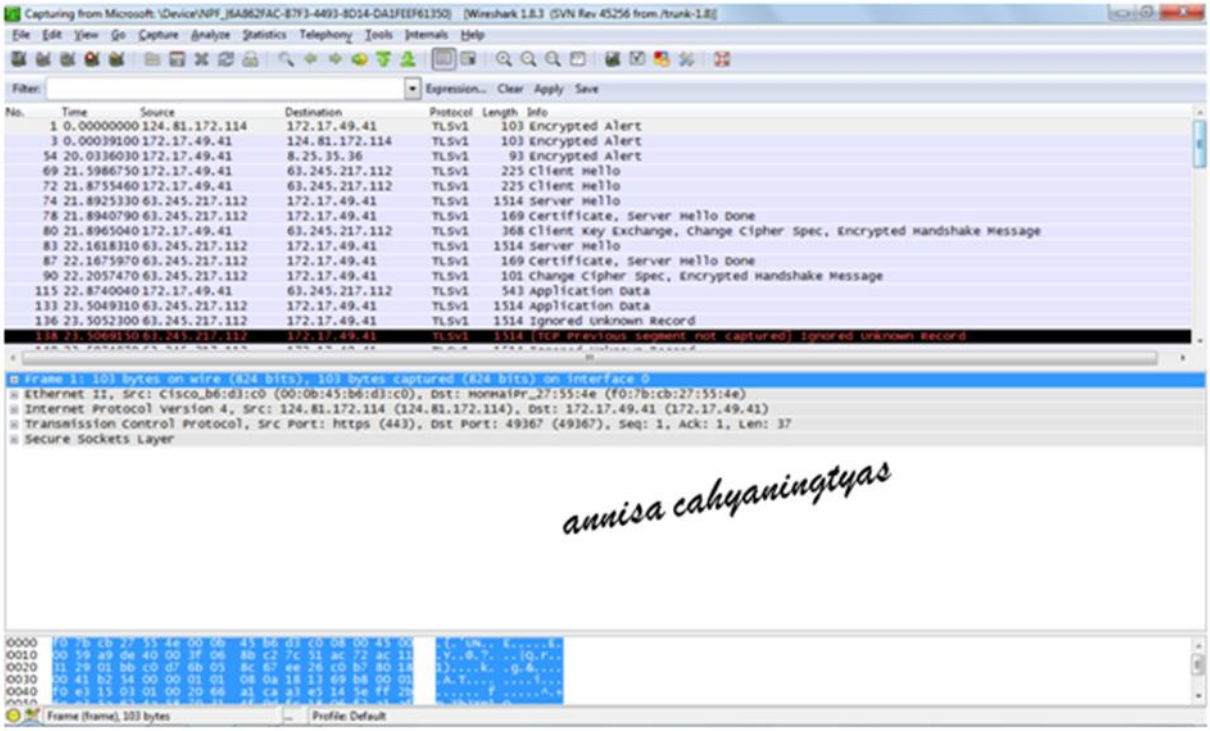
Terdapat dua implementasi SSL: SSLeay dan OpenSSL. Microsoft menerapkan versi SSH-nya sendiri yang dikenal sebagai TLS atau Transport Layer Security (disebut juga sebagai SSL v.3.1), namun tidak mendapat banyak dukungan diluar produk-produk Microsoft sendiri.

5. Monitoring dengan Wireshark

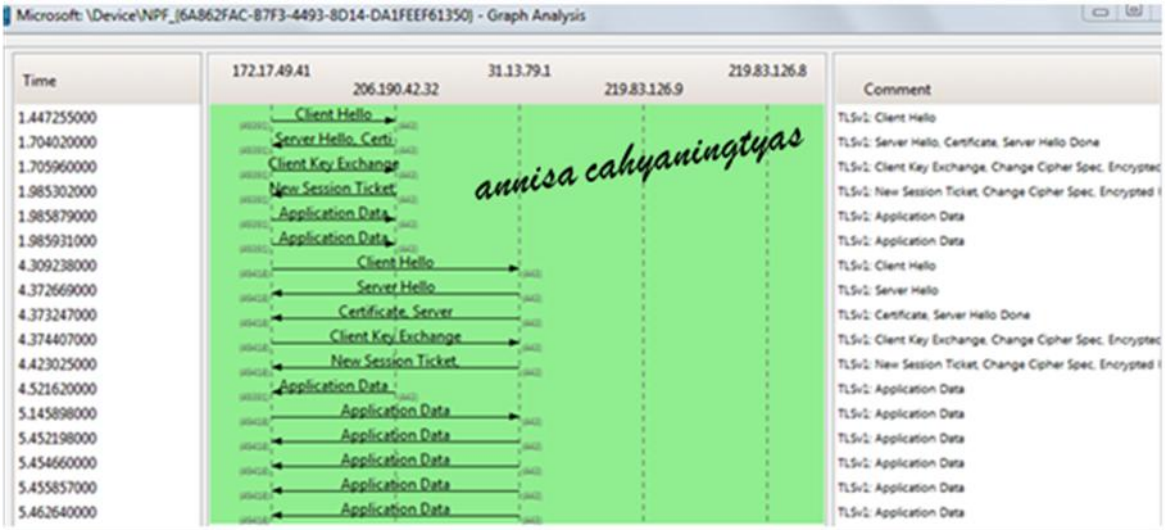
Untuk memonitoring atau mengamati SSL dapat membuka website memakai https. Dan kesempatan ini, akan diakses website https://facebook.com/ . Kemudian akan dilakukan capture lalu lintas pada jaringannya menggunakan wireshark. Setelah dilakukan capture SSL yang tertangkap ternyata protokol TLSV1.

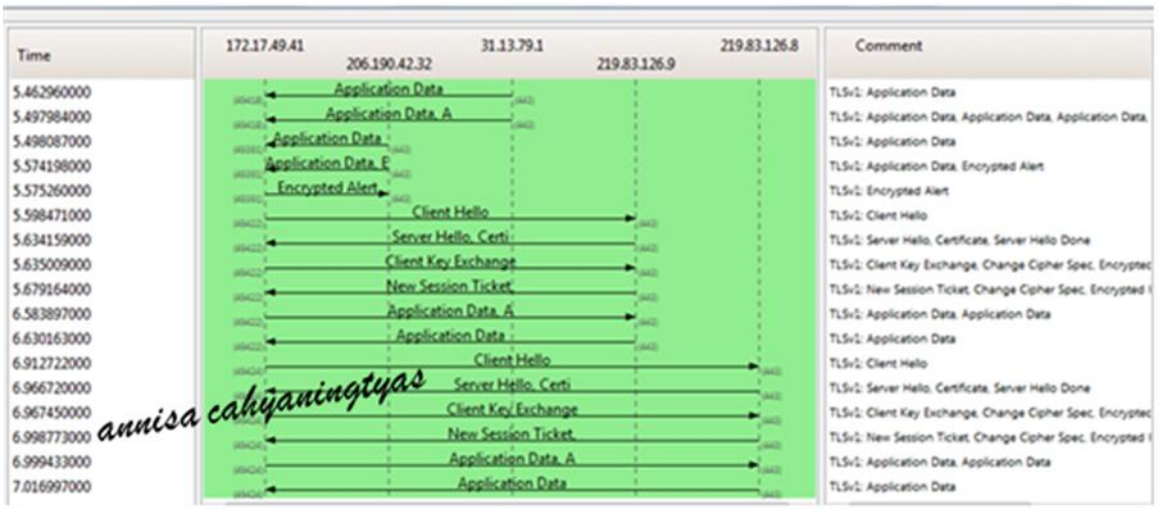
    a. Pertama, membuka web browser kemudian mengakses facebook dengan HTTPS

b. Selanjutnya, menjalankan wireshrak kemudian memilih interface yang aktif dan meng-capture paket data (yang seharusnya SSL, namun yang tertangkap oleh Wireshark adalah TLSv1)



c. Bila ingin mengetahui bagaimana jalannya lalu lintas paket data ataupun flow graph dari paket data yang ada dengan protokol tertentu (untuk monitoring kali ini TLSv1)





Sesuai dengan penjelasan di atas, bahwa salah satu implementasi SSL dalam Microsoft menerapkan versi SSH-nya sendiri yang dikenal sebagai TLS atau Transport Layer Security (disebut juga sebagai SSL v.3.1). Kemudian, telah terpapar gambar capture dari wireshark dan flow graph-nya, berikut sedikit penjelasannya (sama seperti penjelasan cara kerja SSL)

1. Awalnya, client mengirimkan pesan Client Hello untuk mengajukan opsi SSL (pada saat awal akses menggunakan https).
2. Selanjutnya, server memberi respon dengan memilih opsi SSL melalui ServerHello.
3. Selain itu, server juga mengirimkan sertifikat kunci publik pada pesan Certificate.
4. Dan, server mengakhiri bagian negoisasi dengan pesan ServerHelloDone.
5. Kemudian, client mengirimkan informasi session key yang dienkripsi dengan kunci publik server melalui pesan ClientKeyExchange (dienkripsi dengan kunci publik yang disediakan oleh server).

6. Proses selanjutnya, client mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
7. Lalu, client mengirimkan pesan Finished sehingga memungkinkan server mengecek opsi baru yang diaktifkan.
8. Kemudian, server mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
9. Proses terakhir, server mengirimkan pesan Finished sehingga memungkinkan client mengecek opsi baru yang diaktifkan.
10. Maka, terjalin sudah komunikasi data yang diminta oleh client dengan persetujuan server serta pengamanan dengan SSL (ataupun TLSv1)

Biografi Penulis

Annisa Cahyaningtyas. Saat ini sedang menjalani studi D4 di Politeknik Negeri Semarang, Jurusan Teknik Elektro, Program Studi Teknik Telekomunikasi.